Amendments to the Claims:

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

1. (Currently Amended): A method for securing an accessible computer system, the method comprising:

monitoring for connection transactions between multiple access requestors and access providers at a switch that is connected to the access providers and that transfers data to and from the access providers~~, wherein the monitoring includes detecting connection transactions between multiple Internet protocol addresses and the access providers with the switch~~; [[and]]

based on the monitoring, determining, by the switch, whether a cumulative number of connection transactions initiated to more than one of the access providers by an attacking access requestor during a first period of time exceeds a threshold number; and

denying, at the switch, access by [[an]] the attacking access requestor to the access providers in response to a determination that the cumulative ~~when a~~ number of connection transactions initiated to more than one of the access providers by the attacking access requestor ~~through the switch~~ exceeds ~~a configurable~~ the threshold number during [[a]] the first ~~configurable~~ period of time.

2. (Canceled)

3. (Currently Amended): The method as in claim 1, wherein the monitoring further includes counting, using the switch, the number of connection transactions initiated by the access requestors to any of the access providers through the switch during the first ~~configurable~~ period of time.

4. (Currently Amended): The method as in claim 1, wherein:

the ~~monitoring~~ determining further includes comparing, using the switch, the number of connection transactions initiated by the access requestors through the switch during the first ~~configurable~~ period of time to the ~~configurable~~ threshold number~~, and~~

~~denying access by the attacking access requestor to the access providers includes denying, using the switch, access by the attacking access requestor to all of the access providers connected to the switch when the comparison results indicate that the number of connection transactions initiated by the attacking access requestor during the first configurable period of time exceeds the configurable threshold number~~.

5. (Canceled)

6. (Currently Amended): The method as in claim 1, wherein the monitoring further includes counting, using the switch, the cumulative number of connection transactions initiated to any of the access providers by the attacking access requestor ~~Internet protocol addresses~~ during the first ~~configurable~~ period of time such that the cumulative number of connection transactions reflects ~~a cumulative number of~~ connection transactions initiated to [[any]] all of the access providers by the attacking access requestor ~~Internet protocol addresses~~.

7. (Currently Amended): The method as in claim 6, wherein the ~~monitoring~~ determining further includes comparing, using the switch, the cumulative number of connection transactions initiated by the attacking access requestor ~~Internet protocol addresses~~ during the first ~~configurable~~ period of time to the ~~configurable~~ threshold number, and

denying access by the attacking access requestor to the access providers includes denying, using the switch, access by the attacking access requestor to all of the access providers connected to the switch when the comparison results indicate that the cumulative number of connection transactions initiated by ~~the Internet protocol address associated with~~ the attacking access requestor during the first ~~configurable~~ period of time exceeds the ~~configurable~~ threshold number.

8. (Original): The method as in claim 6, wherein the monitoring includes monitoring a computer system for connection transactions made using TCP.

9. (Currently Amended): The method as in claim [[1]] 46, wherein the detecting includes identifying the Internet protocol addresses through the use of a header attached to a message representing [[the]] a connection transaction being detected.

10. (Previously presented): The method as in claim 1, wherein the denying of access includes denying access to the access providers through the switch by the attacking access requestor for a second configurable period of time.

11. (Previously presented): The method as in claim 10, wherein the denying of access further includes resetting the second configurable period of time after detecting a new connection transaction initiated by the attacking access requestor through the switch during the second configurable period of time.

12. (Previously presented): The method as in claim 1, wherein the denying of access includes denying access to the access providers through the switch by the attacking access requestor for a second configurable period of time after detecting a most recent connection transaction initiated by the attacking access requestor through the switch.

13. (Previously presented): The method as in claim 1, wherein the access requestors are clients and the access providers are hosts such that the monitoring includes detecting connection transactions through the switch between multiple clients and multiple hosts.

14. (Currently Amended): The method as in claim 3, wherein the counting further comprises counting, using the switch, a cumulative number of connection transactions for all of the access providers connected to the switch initiated by each of the access requestors during the first ~~configurable~~ period of time.

15-24. (Cancelled)

25. (Currently Amended): A system for securing an accessible computer system, comprising:

a switch that is connected to access providers and that includes at least one hardware component configured to:

monitor for connection transactions between multiple access requestors and access providers~~, wherein to monitor for connection transactions include to detect connection transactions between multiple Internet protocol addresses and the access providers with the switch~~; [[and]]

based on the monitoring, determine whether a cumulative number of connection transactions initiated to more than one of the access providers by an attacking access requestor during a first period of time exceeds a threshold number; and

deny access by the attacking access requestor to the access providers in response to a determination that the cumulative ~~when a~~ number of connection transactions initiated to more than one of the access providers by an attacking access requestor exceed ~~a configurable~~ the threshold number during [[a]] the first ~~configurable~~ period of time.

26. (Currently Amended): The system of claim 25, wherein the switch comprises:

a detection component that is structured and arranged to detect connection transactions initiated by the access requestors through the switch;

a counting component that is structured and arranged to count the number of connection transactions initiated by the access requestors to any of the access providers through the switch during the first ~~configurable~~ period of time;

a comparing component that is structured and arranged to compare the number of connection transactions initiated by the access requestors through the switch during the first ~~configurable~~ period of time to the ~~configurable~~ threshold number; and

the switch is configured to deny access by the attacking access requestor to all of the access providers when the comparison results indicate that the number of connection transactions

initiated by the attacking access requestor during the first ~~configurable~~ period of time exceeds the ~~configurable~~ threshold number.

27. (Currently Amended): The system of claim 25, wherein the switch comprises:

~~a detection component that is structured and arranged to detect connection transactions through the switch between the multiple Internet protocol addresses and the access providers;~~

a counting component that is structured and arranged to count the cumulative number of connection transactions to any of the access providers initiated through the switch by the ~~Internet protocol addresses~~ attacking access requestor during the first ~~configurable~~ period of time such that the cumulative number of connection transactions reflects ~~a cumulative number of~~ connection transactions initiated to [[any]] all of the access providers by the ~~Internet protocol addresses~~ attacking access requestor;

a comparing component that is structured and arranged to compare the cumulative number of connection transactions initiated through the switch by the ~~Internet protocol addresses~~ attacking access requestor during the first ~~configurable~~ period of time to the ~~configurable~~ threshold number; and

the switch is configured to deny access by the attacking access requestor to all of the access providers when the comparison results indicate that the cumulative number of connection transactions initiated by the ~~Internet protocol address associated with the~~ attacking access requestor during the first ~~configurable~~ period of time exceeds the ~~configurable~~ threshold number.

28. (Original): The system of claim 27, wherein the connection transactions include connections made using TCP.

29. (Currently Amended): The system of claim 27, further comprising ~~wherein the detection component comprises~~:

an identifying component that is structured and arranged to identify [[the]] Internet protocol addresses through the use of a header attached to a message representing [[the]] a connection transaction being detected.

30. (Previously presented): The system of claim 25, wherein the switch comprises:

an access preventer that is structured and arranged to deny access to the access providers through the switch by the attacking access requestor for a second configurable period of time.

31. (Previously presented): The system of claim 30, wherein the switch further comprises:

a timing component that is structured and arranged to measure the second configurable period of time during which the access preventer denies access to the access providers by the attacking access requestor.

32. (Previously presented): The system of claim 31, wherein the switch further comprises:

a reset component that is structured and arranged to reset the timing component after detecting a new connection transaction initiated by the attacking access requestor through the switch during the second configurable period of time.

33. (Previously presented): The system of claim 25, wherein the switch comprises:

an access preventer that is structured and arranged to deny access to the access providers through the switch by the attacking access requestor for a second configurable period of time after detecting a most recent connection transaction initiated by the access requestor.

34. (Previously presented): The system of claim 25, wherein the access requestors are clients and the access providers are hosts such that the switch comprises:

a detection component that is structured and arranged to detect connection transactions through the switch between multiple clients and multiple hosts.

35. (Currently Amended): The system of claim 26, wherein the counting component further comprises counting a cumulative number of connection transactions for all of the access providers connected to the switch initiated by each of the access requestors during the first ~~configurable~~ period of time.

36. (Previously presented): The system of claim 25, wherein a host computer system receives communications from the switch.

37. (Previously presented): The system of claim 25, wherein the switch is included in a host computer system.

38. (Currently Amended): The method of claim 1 wherein denying access by the attacking access requestor to the access providers ~~when the number of connection transactions initiated by the attacking access requestor through the switch exceeds a configurable threshold number during the first configurable period of time~~ comprises denying, using the switch, access by the attacking access requestor to all of the access providers connected to the switch irrespective of which of the access providers to which the attacking access requestor initiated connection transactions to exceed the ~~configurable~~ threshold.

39. (Previously Presented): The method of claim 1 wherein the monitoring includes monitoring, using a switch configured to establish communication links between access requestors and access providers, for attempts, by the attacking access requestor, to establish a communication link with any of the access providers.

40. (Previously Presented): The method of claim 39 wherein monitoring for attempts, by the attacking access requestor, to establish a communication link with any of the access providers includes monitoring for attempts, by the attacking access requestor, to establish a communication link with any of the access providers, the establishment of a communication link between the attacking access requestor and one of the access providers involving exchange of more than two electronic messages.

41. (Previously Presented): The method of claim 11 further comprising:

determining, using the switch, that the second configurable time period has passed without detecting a new connection transaction initiated by the attacking access requestor to any of the access providers through the switch; and

in response to determining that the second configurable time period has passed without detecting a new connection transaction initiated by the attacking access requestor to any of the access providers through the switch, allowing access by an attacking access requestor to the access providers.

42-44. (Cancelled)

45. (Previously Presented) The method of claim 1 wherein:

the access providers include a first access provider and a second access provider that is different from the first access provider, and

the monitoring takes into account interactions of the attacking access requestor with both the first access provider and second access provider.

46. (New) The method of claim 1 wherein the monitoring includes detecting connection transactions between multiple Internet protocol addresses and the access providers with the switch.

47. (New) The method of claim 1 wherein determining, by the switch, whether the cumulative number of connection transactions initiated to more than one of the access providers by the attacking access requestor during the first period of time exceeds the threshold number comprises determining, by the switch, whether a cumulative number of connection transactions initiated to more than one of the access providers by the attacking access requestor during a first configurable period of time exceeds a configurable threshold number.

48. (New) The method of claim 1 wherein determining, by the switch, whether the cumulative number of connection transactions initiated to more than one of the access providers by the attacking access requestor during the first period of time exceeds the threshold number comprises determining, by the switch, whether a total number of connection transactions initiated to all of the access providers by the attacking access requestor during the first period of time exceeds the threshold number.

49. (New) The method of claim 1 wherein determining, by the switch, whether the cumulative number of connection transactions initiated to more than one of the access providers by the attacking access requestor during the first period of time exceeds the threshold number comprises determining that the cumulative number of connection transactions exceeds the threshold number despite a number of connection transaction initiated to each of the more than one of the access providers individually being less than the threshold number.

50. (New) A switch comprising:

a processor; and

a memory encoded with machine readable instructions that, when executed by the processor, operate to cause the processor to perform operations comprising:

transferring data to and from access providers;

monitoring, at the switch, for connection transactions between multiple access requestors and the access providers;

based on the monitoring, determining, by the switch, whether a cumulative number of connection transactions initiated to more than one of the access providers by an attacking access requestor during a first period of time exceeds a threshold number; and

denying, at the switch, access by the attacking access requestor to the access providers in response to a determination that the cumulative number of connection transactions initiated to more than one of the access providers by the attacking access requestor exceeds the threshold number during the first period of time.

51. (New) The switch of claim 50, wherein the monitoring further includes counting, using the switch, the cumulative number of connection transactions initiated to any of the access providers by the attacking access requestor during the first period of time such that the cumulative number of connection transactions reflects connection transactions initiated to all of the access providers by the attacking access requestor.

52. (New) The switch of claim 51, wherein the determining further includes comparing, using the switch, the cumulative number of connection transactions initiated by the attacking access requestor during the first period of time to the threshold number, and

denying access by the attacking access requestor to the access providers includes denying, using the switch, access by the attacking access requestor to all of the access providers connected to the switch when the comparison results indicate that the cumulative number of connection transactions initiated by the attacking access requestor during the first period of time exceeds the threshold number.

53. (New) The switch of claim 50, wherein the denying of access includes denying access to the access providers through the switch by the attacking access requestor for a second configurable period of time.

54. (New) The switch of claim 53, wherein the denying of access further includes resetting the second configurable period of time after detecting a new connection transaction initiated by the attacking access requestor through the switch during the second configurable period of time.

55. (New) The switch of claim 50 wherein the monitoring includes detecting connection transactions between multiple Internet protocol addresses and the access providers with the switch.

56. (New) The switch of claim 50 wherein determining, by the switch, whether the cumulative number of connection transactions initiated to more than one of the access providers by the attacking access requestor during the first period of time exceeds the threshold number comprises determining, by the switch, whether a cumulative number of connection transactions initiated to more than one of the access providers by the attacking access requestor during a first configurable period of time exceeds a configurable threshold number.

57. (New) The switch of claim 50 wherein determining, by the switch, whether the cumulative number of connection transactions initiated to more than one of the access providers by the attacking access requestor during the first period of time exceeds the threshold number comprises determining, by the switch, whether a total number of connection transactions initiated to all of the access providers by the attacking access requestor during the first period of time exceeds the threshold number.

58. (New) The switch of claim 50 wherein determining, by the switch, whether the cumulative number of connection transactions initiated to more than one of the access providers by the attacking access requestor during the first period of time exceeds the threshold number comprises determining that the cumulative number of connection transactions exceeds the threshold number despite a number of connection transaction initiated to each of the more than one of the access providers individually being less than the threshold number.